UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,518	04/01/2004	David Fultz	IDF 2564 (4000-15700)	8230

28003 7590 03/11/2010

SPRINT
6391 SPRINT PARKWAY
KSOPHT0101-Z2100
OVERLAND PARK, KS 66251-2100

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	**PAPER NUMBER**
2436	
MAIL DATE	**DELIVERY MODE**
03/11/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/815,518	FULTZ ET AL.	
	Examiner	Art Unit	
	SHANTO M. ABEDIN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28 and 30-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *28 and 30-33* is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/28/2009 has been entered.

2. Claims 1-28 and 30-33 have been presented for examination.

3. Claims 28 and 30-33 have been allowed.

4. Claims 1-27 have been rejected.

Response to Arguments

5. The applicant's arguments regarding 35 USC 103(a) type rejections of claims 1-27 are fully considered, however, moot in view of the new grounds of rejection presented in this office action.

6. The applicant's arguments regarding objections to claims 1-8, 13-14, 28 and 30-33 are fully considered. The previous objections to claims 1-8, 14, 28 and 30-33 are withdrawn because of the amendments made to the claims. The objections to claim 13 are maintained since amendments failed to overcome the issues regarding the previous objections (please see the office action below.)

Claim Objections

7. Claim 13 is objected to because of the following informalities:

Regarding claim 13, it recites the limitations such as "wherein information related to the token comprises the token", however, phrase "the token comprises the token" found to be indefinite or

ambiguous in nature! The applicant is suggested to rewrite the claim to include limitations similar to "the information related to the token is the token itself" (please also see Par 016 of the specification) to increase the clarity of the claim languages.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-8 are rejected under 35 U.S.C. 102(e) as anticipated by US 2005/0108521 A1 (Silhavy et al) or, in the alternative, under 35 U.S.C. 103(a) as obvious over US 7178163 B2 (Reeves, Jr)

Regarding claim 1, Silhavy et al discloses a system to provide application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the applications to another (Fig 3.310 and 3.330; Par 007, 019, 034; multi-platform sign in mechanism; creating new context upon invocation of an application), the system comprising:

a first computer comprising a security application program interface (Fig 2.208a; Par 023, 026; client system comprising security service) and an application program interface coupled to a client application on a first platform, the security application program interface operable to provide a security credential (Par 028, 030, 035-036; client system providing credentials);

an authentication authority (Par 026, 028, 035-036; authentication authority; KDC/ Kerberos) receiving the security credential from the security application program interface, the authentication authority further generates a token and communicates the token to the security application program interface where the security credential is valid (Par 029, 023, 034, 039-040; authentication authority/ Kerberos server for generating token/ service ticket; client security services obtaining token/ service ticket from the credential server), wherein the token contains user credentials encoded as a platform and application independent string data type (Par 005, 019, 022, 028; driver is capable of facilitating a secure context regardless of the operating system)

a store maintaining data validating the security credential, the store in communication with the authentication authority to validate the security credential (Par 026, 028, 034-036; database/ server in communication with the authentication authority/ server for credential authentication),

the application program interface communicating regarding the validity of the token (Par 023, 028, 036, 040; ticket/ token validation messages); and

a second computer (Par 028, 036, 040-041; server) comprising a distinct server application on a second platform to receive the token from the application program interface, the server application communicating with the authentication authority to validate the token to enable the client application to use services of the server application (Par 028, 034-036, 039-041; accessing application upon token validation) , wherein there is no continuing context or session and a new context is created with an invocation of the distinct server application by the client application (Fig 3.310 and 3.330; Par 007, 034; creating new context upon invocation of an application)

Although, Silhavy et al's teachings of platform independent driver, and use of security context regardless of the operating system (Par 005, 019, 022, 028; driver is capable of facilitating a secure

context regardless of the operating system) teaches enablement of wherein the token contains user credentials encoded as a platform and application independent string data type, in the case, position regarding the inherency of the above teachings were not found supportable, Reeves, Jr. alternatively teaches wherein the token contains user credentials encoded as a platform and application independent string data type (Col 7, starts at line 44; XML encoded token; platform independent languages such as XML)

Reeves, Jr. and Silhavy et al's are analogous art because they are from the same field of endeavor of cross platform authentication. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teaching of Reeves, Jr. with Silhavy et al to design a system wherein the token contains user credentials encoded as a platform and application independent string data type in order to facilitate a cross platform authentication mechanism using XML security credential.

Regarding claim 2, it is rejected applying as above applied rejecting claim 1, furthermore, Silhavy et al teaches the system wherein the server application further comprises:

an application program interface to communicate with the application program interface of the client application (Fig 2.202.b; Par 022-023, 027-028; server communication interface); and

a security application program interface to communicate with the authentication authority (Fig 2.160; Par 023, 028; server security mechanism.)

Regarding claim 3, it is rejected applying as above applied rejecting claim 1, furthermore, Silhavy et al teaches the system wherein the server application caches the token after validating the token with the authentication authority such that when the client application requests service of the server application, via the application program interfaces of the client application, the server application uses the cached token to validate the client application (Par 035-039; server using cached credential/ token).

Regarding claim 4, it is rejected applying as above applied rejecting claim 1, furthermore, Reeves, Jr. teaches the system wherein the token generated by the authentication authority comprises a string including at least a portion of the security credential (Col 7, starts at line 44; XML encoded token comprising string/ text.)

Regarding claim 5, it is rejected applying as above applied rejecting claim 1, furthermore, Reeves, Jr. teaches system wherein at least a portion of the token is in Extensible Markup Language format (Col 7, starts at line 44; XML encoded token.)

Regarding claim 6, modified Reeves, Jr.-Silhavy et al method fails to teach wherein at least a portion of the token is in Security Assertion Markup Language format. However, the examiner takes an official notice on that at the time of invention, generating at least a portion of the token in Security Assertion Markup Language format was well known in art (Please see US 7,444,519, Laferriere et al; US 7313812 B2, Robinson et al.) Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to design a system wherein at least a portion of the token is

generated in Security Assertion Markup Language format in order to provide an alternative mechanism for generating security context.

Regarding claim 7, Reeves, Jr. teaches the system wherein the token includes information related to an expiration date of the token (Fig 4.402; Col 8, starts at line 16; time-stamp in ticket/ token).

Regarding claim 8, Silhavy et al teaches the system wherein validating the token by the authentication authority includes determining whether the authentication authority created the token (Col 7, starts at line 45; XML encoded token; authorization/ Operator information in token)

9. Claims 9-27 are rejected under 35 USC 103 (a) as being unpatentable over Bhatia et al (US 7,249,375 B2) in view of Silhavy et al (US 2005/0108521 A1) further in view of US 7178163 B2 (Reeves, Jr)

Regarding claim 9, Bhatia et al discloses a method for providing application-to-application enterprise security for different applications on different platforms, the method comprising:

coupling a security application program interface and an application program interface to a client application on a first platform (Fig 1.102; Col 3, starts at line 16; user application);

communicating a security credential from the security application program interface to an authentication authority (Col 3, starts at line 16; user sending access request to SSO server);

communicating information related to the security credential between the authentication authority and a data store to determine whether the security credential is valid (Col 3, starts at line 16; SSO server authenticating user credentials/ identity);

generating a token by the authentication authority when the security credential is valid (Fig 3; Col 3, lies 16-25, and 55-62; generating, and providing security token upon user authentication), wherein the token contains user credentials encoded as a platform and application independent string data type (Fig 3; Col 3, starts at line 16; XML/ security token for authentication; XML token is interpreted as platform independent credential);

providing, by the application program interface coupled to the client application on the first platform, the token to a distinct server application, the distinct server application on a second platform (Col 3, starts at line 12; providing token to the backend server, or RDBMS to access applications);

validating, by the server application, the token before providing access to services of the distinct server application by the client application (Fig 1, Fig 3; Col 3, starts at line 16; SSO enabled front end services uses token to access the backend-tier applications)

Although Bhatia et al teaches communicating the token to the application service (Col 3, lines 45-65), it fails to disclose expressly communicating the token to the client application; and wherein there is no continuing context or session and a new context is created with an invocation of the distinct server application by the client application.

However, Silhavy et al discloses communicating the token to the client application (Par 029, 023, 034, 039-040; authentication authority/ Kerberos server for generating token/ service ticket; client security services obtaining token/ service ticket from the credential server); and wherein there is no continuing context or session and a new context is created with an invocation of the distinct server

application by the client application (Fig 3.310 and 3.330; Par 007, 034; creating new context upon invocation of an application).

In the case, position regarding the inherency of the above teachings (such as the token contains user credentials encoded as a platform and application independent string data type) were not found supportable, Reeves, Jr. alternatively teaches wherein the token contains user credentials encoded as a platform and application independent string data type (Col 7, starts at line 44; XML encoded token; platform independent languages such as XML)

Reeves, Jr. , Silhavy et al and Bhatia et al are analogous art because they are from the same field of endeavor of cross platform authentication. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teaching of Reeves, Jr. with the modified Silhavy et al- Bhatia et al method to further include the token containing user credentials encoded as a platform and application independent string data type in order to facilitate a robust cross platform authentication mechanism using XML security credential.

Regarding claim 10, it is rejected applying as above applied rejecting claim 9, furthermore, Bhatia et al discloses the method wherein the distinct server application is provided with a security application program interface coupled to the distinct server application for validating the token with the authentication authority (Fig 1; Col 3, starts at line 45; RDBMS, or application services for validating the token with the SSO server.)

Regarding claim 11, it is rejected applying as above applied rejecting claim 9, furthermore, Bhatia et al discloses the method wherein the application program interface coupled to the client

application communicates the token to an application program interface of the distinct server application (Col 3, starts at line 3; user application).

Regarding claim 12, it is rejected applying as above applied rejecting claim 9, furthermore, Bhatia et al discloses the method wherein validating the token by the distinct server application further comprises:

communicating information related to the token to the authentication authority (Fig 1; Col 3, starts at line 45; RDBMS, or application services for validating the token with the SSO server, or the credential/ token provider);

determining, by the authentication authority, whether the token is authentic (Fig 2; Col 3, starts at line 45; determining by the SSO server/ token provider whether token is authentic); and

receiving validation related information from the authentication authority (Fig 2; Col 3, starts at line 53; RDBMS receiving information about the token/ credential validity).

Regarding claim 16, it is rejected applying as above applied rejecting claim 9, furthermore, Bhatia et al discloses the method wherein the authentication authority determines whether token is expired (Col 3, starts at line 25; verifying SSO session specific tokens)

Regarding claim 18, it is rejected applying as above applied rejecting claim 9, furthermore, Bhatia et al discloses wherein the token includes a portion of the security credential in a string format (Col 3, starts at line 55; standard XML token)

Regarding claim 20, it is rejected applying as above applied rejecting claims 9 and 18. Furthermore, Bhatia et al fails to disclose using the encrypted token. However, the examiner takes an official notice on that at the time of invention, using encrypted token for authentication purposes was well known in the art (See Bhat et al , US 2003/0200465 A1.) Therefore, it would have been obvious to a person of ordinary skill in the art to utilize the encrypted token for authentication purposes in order to provide better credential security.

Regarding claim 24, Bhatia et al discloses wherein the security credential is further defined as including a password and user identification (Col 3, starts at line 56; name/ password for user authentication).

Regarding claim 25, it recites the limitations of claim20 and 24, therefore, it is rejected applying as above rejecting claims 20 and 24.

Regarding claim 26, Bhatia et al discloses the method wherein the security credential is an X.509 certificate and the data store is a certificate authority (Col 3, starts at line 55; use of certificates as credentials)

Regarding claims 13-15, 17, 19, 21-23, they recite the limitations of claims 9-12, 16, 18 and 20, therefore, they are rejected applying as above applied rejecting claims 9-12, 16, 18 and 20.

Regarding claim 27, it is rejected applying as above applied rejecting claims 9 and 26, furthermore, Bhatia et al discloses the method further comprising: communicating the X.509 certificate from the authentication authority to the certificate authority (Col 3, starts at line 55; SSO server or RDBMS optionally using token including PKI certificate); validating the X.509 certificate by the certificate authority (Fig 3; Col 3, starts at line 45; validating the token/ PKI certificate); and communicating validation information to the authentication authority (Col 3, starts at line 45; communicating the token/ certificate validation to the SSO server or back-tier application services).

Allowable Subject Matter

10. Claims 28 and 30-33 have been allowed.

Conclusion

11. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 10:00 AM to 6:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained

from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, A.U. 2436

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436